

## CLAIMS

What is claimed is:

- 1    1.    A method for computing a group shared secret key at a first node of a network for use  
2        in a public key process and using less than  $n * (n-1)$  messages, where “n” is a number  
3        of nodes in a broadcast or multicast group of the network, the method comprising the  
4        computer-implemented steps of:  
5        generating an intermediate shared secret key by issuing communications to a second  
6            node of the network;  
7        sending a first private value associated with the first node to the second node, and  
8            receiving from the second node a second private value associated with the  
9            second node using the intermediate shared secret key;  
10       generating and communicating a collective public key that is based upon the first  
11           private value and the second private value to a third node of the network;  
12       receiving an individual public key from the third node; and  
13       computing and storing the group shared secret key based upon the individual public  
14           key.
- 1    2.    The method as recited in Claim 1, further comprising:  
2        joining the first node to an initial multicast group in response to generating the  
3            intermediate shared secret key; and  
4        joining a second node to a new multicast group that subsumes the initial multicast  
5            group after receiving the individual public key.
- 1    3.    The method as recited in Claim 1, wherein the public-key process is Diffie-Hellman  
2        key exchange.
- 1    4.    The method as recited in Claim 1, wherein the step of communicating the collective  
2        public key further comprises determining whether the first node or the second node  
3        transfers the collective public key based upon an order of entry of such nodes into a  
4        multicast group.

- 1 5. The method as recited in Claim 1, wherein the step of communicating the collective  
2 public key further comprises determining whether the first node or the second node  
3 transfers the collective public key based upon a predetermined metric.
- 1 6. The method as recited in Claim 1, wherein sending the first private value and  
2 receiving the second private value further comprises computing the first private value  
3 as a random integer and receiving a second random integer as the second private  
4 value.
- 1 7. The method as recited in Claim 1, further comprising creating and storing information  
2 at the first node that associates the first node, the second node, and the third node as a  
3 multicast group communicating over a packet switched network.
- 1 8. The method as recited in Claim 1, wherein the steps of generating, sending,  
2 communicating, and receiving further comprise communicating approximately  $2n +$   
3  $2(n-1)$  total messages.
- 1 9. The method as recited in Claim 1, wherein the step of communicating the collective  
2 public key comprises storing the collective public key and receiving the collective  
3 public key using a key distribution center.
- 1 10. The method as recited in Claim 1, further comprising the step of establishing a  
2 cryptographic communication session between the first node and the second node,  
3 whereby secure communications are established between the first and the second node  
4 using public key exchange and only approximately  $2n + 2(n-1)$  total messages.
- 1 11. A method as recited in Claim 1, wherein generating the shared secret key value  
2 comprises computing and storing the shared secret key value "k" at the first node  
3 according to the relation  
4 
$$k = C^{ab} \bmod (q) = p^{abc} \bmod (q)$$
  
5 wherein C, a, b, c, q, and p are values stored in a memory, and wherein C is the  
6 individual public key, a is the private value of the first node, b is the private

7 value of the second node, c is a third private value of the third node, p is a  
8 base value, and q is a prime number value.

- 1 12. A method for exchanging cryptographic keys among a plurality of nodes in a  
2 multicast or broadcast group, the method comprising the computer-implemented steps  
3 of:  
4 (a) computing and storing a first shared secret key at a first node;  
5 (b) transmitting a first message, encrypted using the first shared secret key, to a  
6 second node;  
7 (c) receiving a second message, encrypted using the first shared secret key, from the  
8 second node;  
9 (d) computing and storing a first public key based upon the first and second  
10 messages;  
11 (e) transmitting the first public key to a third node;  
12 (f) receiving a second public key from the third node;  
13 (g) computing a second shared secret key based upon the second public key, the first  
14 message, and the second message;  
15 (h) iteratively performing steps of (e) through (g) until the nodes reach a group shared  
16 secret key for use in cryptographic communication among the of nodes, and  
17 using less than  $n * (n-1)$  total messages;  
18 whereby the first node and second node independently come to a shared secret key  
19 value.

- 1 13. The method as recited in Claim 12, further comprising:  
2 joining the first node to an initial multicast group in response to generating the first  
3 public key; and  
4 joining the first node to a new multicast group that subsumes the initial multicast  
5 group after receiving the second public key.

- 1 14. The method as recited in Claim 12, wherein the step of transmitting the first public  
2 key further comprises determining whether the first node or the second node transfers  
3 the first public key based upon an order of entry of such nodes into a multicast group.

- 1 15. The method as recited in Claim 12, further comprising creating and storing  
2 information at the first node that associates the first node, the second node, and the  
3 third node as a multicast group communicating over a packet switched network.
- 1 16. The method as recited in Claim 12, wherein step (h) comprises the step of:  
2 (h) iteratively performing steps of (e) through (g) until the nodes reach a group shared  
3 secret key for use in cryptographic communication among the of nodes, and  
4 using approximately  $2n + 2(n-1)$  total messages.
- 1 17. The method as recited in Claim 12, further comprising communicating with a key  
2 distribution center to obtain public keys for use in arriving at a shared secret value.
- 1 18. The method as recited in Claim 12, further comprising the step of establishing a  
2 cryptographic communication session between the nodes, whereby secure  
3 communications are established between the nodes using public key exchange and  
4 only approximately  $2n + 2(n-1)$  total messages.
- 1 19. A method as recited in Claim 12, wherein generating the shared secret key value  
2 comprises computing and storing the first shared secret key value "k" at the first node  
3 according to the relation  
4 
$$k = C^{ab} \bmod (q) = p^{abc} \bmod (q)$$
  
5 wherein C, a, b, c, q, and p are values stored in a memory, and wherein C is the  
6 individual public key, a is the private value of the first node, b is the private  
7 value of the second node, c is a third private value of the third node, p is a  
8 base value, and q is a prime number value.

1 20. A computer-readable medium carrying one or more sequences of one or more  
2 instructions for computing a group shared secret key at a first node of a network for  
3 use in a public key process and using less than  $n * (n-1)$  messages, where “n” is a  
4 number of nodes in a broadcast or multicast group of the network, and which  
5 instructions, when executed by one or more processors, cause the one or more  
6 processors to perform the steps of:  
7 generating an intermediate shared secret key by issuing communications to a second  
8 node of the network;  
9 sending a first private value associated with the first node to the second node, and  
10 receiving from the second node a second private value associated with the  
11 second node using the intermediate shared secret key;  
12 generating and communicating a collective public key that is based upon the first  
13 private value and the second private value to a third node of the network;  
14 receiving an individual public key from the third node; and  
15 computing and storing the group shared secret key based upon the individual public  
16 key.

1 21. The computer-readable medium recited in Claim 20, wherein the instructions further  
2 cause the one or more processors to carry out the steps of:  
3 joining the first node to an initial multicast group in response to generating the  
4 intermediate shared secret key; and  
5 joining the first node to a new multicast group that subsumes the initial multicast  
6 group after receiving the individual public key.

1 22. The computer-readable medium as recited in Claim 20, wherein the public-key  
2 process is Diffie-Hellman key exchange.

1 23. The computer-readable medium as recited in Claim 20, wherein the instructions for  
2 communicating the collective public key further comprise instructions for determining  
3 whether the first node or the second node transfers the collective public key based  
4 upon an order of entry of such nodes into a multicast group.

- 1 24. The computer-readable medium as recited in Claim 20, wherein the instructions for  
2 communicating the collective public key further comprise instructions for determining  
3 whether the first node or the second node transfers the collective public key based  
4 upon a predetermined metric.
- 1 25. The computer-readable medium as recited in Claim 20, wherein the instructions for  
2 sending the first private value and receiving the second private value further comprise  
3 instructions for computing the first private value as a random integer and receiving a  
4 second random integer as the second private value.
- 1 26. The computer-readable medium as recited in Claim 20, further comprising  
2 instructions for creating and storing information at the first node that associates the  
3 first node, the second node, and the third node as a multicast group communicating  
4 over a packet switched network.
- 1 27. The computer-readable medium as recited in Claim 20, wherein the instructions for  
2 generating, sending, communicating, and receiving further comprise instructions that  
3 communicate only approximately  $2n + 2(n-1)$  total messages.
- 1 28. The computer-readable medium as recited in Claim 20, wherein the instructions for  
2 communicating the collective public key further comprise instructions for storing the  
3 collective public key and receiving the collective public key using a key distribution  
4 center.
- 1 29. The computer-readable medium as recited in Claim 20, further comprising  
2 instructions for establishing a cryptographic communication session between the first  
3 node and the second node, whereby secure communications are established between  
4 the first and the second node using public key exchange and only approximately  $2n +$   
5  $2(n-1)$  total messages.

1 30. A computer-readable medium as recited in Claim 20, wherein the instructions for  
2 generating the shared secret key value further comprise instructions for computing  
3 and storing the shared secret key value “k” at the first node according to the relation

4 
$$k = C^{ab} \bmod (q) = p^{abc} \bmod (q)$$

5 wherein C, a, b, c, q, and p are values stored in a memory, and wherein C is the  
6 individual public key, a is the private value of the first node, b is the private  
7 value of the second node, c is a third private value of the third node, p is a  
8 base value, and q is a prime number value.